PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Douglas R. Coffland, et al.	Docket No. :	IL-10360
Serial No. :	09/405,031	Art Unit :	2164
Filed :	09/24/1999	Examiner :	Jacob F. Betit
For :	SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION		

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

Dear Sir:

APPELLANTS' AMENDED BRIEF (37 C.F.R. § 1.192)
(Responsive to 01/26/2009 Notification of Non-Compliant Appeal Brief)

This brief is submitted in support of Appellants' notice of appeal from the decision of the Examiner, mailed April 25, 2008 finally rejecting claims 1-30 of the subject application. Appellants' notice of appeal was mailed July 24, 2008.

One copy of the brief is being transmitted per 37 C.F.R. § 41.37.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is:

Lawrence Livermore National Security, LLC and the United States of America as represented by the United States Department of Energy (DOE) by virtue of an assignment by the inventor as duly recorded in the Assignment Branch of the U.S. Patent and Trademark Office.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

The application as originally filed contained claims 1-30.

The claims on appeal are claims 1-30.

The status of all the claims in the proceeding (*e.g.*, rejected, allowed or confirmed, withdrawn, objected to, canceled) is:

Claims 1-30 are rejected.

Claims 1-30 on appeal are reproduced in the Appendix.

IV. STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the Final Rejection mailed April 25, 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants' invention includes a method with the steps of acquiring a random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise; compressing said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise; selecting a set of data from the compressed media signal; and hashing the set of data into a keyword. This is described in Appellants' original specification as follows: "A data compression module receives and compresses a media signal into a compressed data stream. A data acquisition module receives and selects a set of data from the compressed data stream. And, a hashing module receives and hashes the set of data into a keyword."(Page 4, lines 2-7)

Appellants' invention provides a system for multimedia encryption comprising: acquisition means for acquiring a media signal, said acquisition means including a random noise transducer for acquiring random noise only, said random noise being unpredictable from one moment to the next and not being chaotic noise; data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise into a compressed data stream; data acquisition means coupled to said data compression means to receive and select a set of data from the compressed data stream; and hashing means coupled to said data acquisition means to receive and hash the set of data into a keyword. FIG. 1 (Reproduced Below) is a block diagram of a system 100 for multimedia encryption according to the invention.

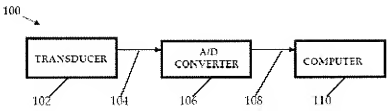


FIG. 1

"In the system 100, a transducer 102, such as a video camera, a radio, a microphone, a Geiger counter, or an electrical component, outputs a media signal 104." (Page 7, lines 2-5) Appellants' means plus function claim elements are identified and the structure described in the specification as corresponding to each claimed function are set forth with reference to the specification by page and line number. ".... the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods." (Page 7, lines 10-15) "The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108." (Page 7, lines 19-22) "Figure 2 is a graphical depiction of quantization processes within the analog-to-digital converter 106 within the system 100. The media signal 104 is periodically sampled 202." (Page 8, lines 2-4) "And, a hashing module receives and hashes the set of data into a keyword. (Page 4, lines 6-7) a hashing module coupled to receive and hash the set of data into a keyword." (Original Claim 1 lines 7-8, Page 14)

The elements of Appellants' independent claims 1, 10, 17, and 24 are "read on" Appellants' original specification as set out below.

Claim 1	Specification & Drawings
1. A system adapted for use for multimedia encryption	Figure 1 is a block diagram of a system 100 for multimedia encryption according to the present invention. (Page 7, lines 2-3)
acquisition means for acquiring a media signal, said acquisition means including a random noise transducer for acquiring random noise only, said random noise being unpredictable from one moment to the next and not being chaotic noise;	In one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods. (Page 7, lines 10-15)
data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise into a compressed data stream;	The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108. (Page 7, lines 19-22)
data acquisition means coupled to said data compression means to receive and select a set of data from the compressed data stream; and	Figure 2 is a graphical depiction of quantization processes within the analog-to-digital converter 106 within the system 100. The media signal 104 is periodically sampled 202. (Page 8, lines 2-4)
hashing means coupled to said data acquisition means to receive and hash the set of data into a keyword.	And, a hashing module receives and hashes the set of data into a keyword. (Page 4, lines 6-7) a hashing module coupled to receive and hash the set of data into a keyword. (Original Claim 1 lines 7-8, Page 14)

Claim 10	Specification & Drawings

10. A method adapted for use for multimedia encryption, comprising the steps of:	Figure 1 is a block diagram of a system 100 for multimedia encryption according to the present invention. (Page 7, lines 2-3)
acquiring a random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;	In one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods. (Page 7, lines 10-15)
compressing said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;	The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108. (Page 7, lines 19-22)
selecting a set of data from the compressed media signal; and	Figure 2 is a graphical depiction of quantization processes within the analog-to-digital converter 106 within the system 100. The media signal 104 is periodically sampled 202. (Page 8, lines 2-4)
hashing the set of data into a keyword.	And, a hashing module receives and hashes the set of data into a keyword. (Page 4, lines 6-7) a hashing module coupled to receive and hash the set of data into a keyword. (Original Claim 1 lines 7-8, Page 14)

Claim 17	Specification & Drawings
17. A system adapted for use for multimedia encryption,	Figure 1 is a block diagram of a system 100 for multimedia encryption according to the present invention. (Page 7, lines 2-3)
acquisition means for acquiring a media signal, said acquisition means including a random noise transducer for acquiring said media signal, said random noise transducer acquiring said media signal containing only random noise that is unpredictable from one moment to the next and not being chaotic noise;	In one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods. (Page 7, lines 10-15)
data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is unpredictable from one moment to the next into a compressed data stream;	The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108. (Page 7, lines 19-22)
selection means coupled to said data compression means for selecting a set of data from the compressed data stream; and	Figure 2 is a graphical depiction of quantization processes within the analog-to-digital converter 106 within the system 100. The media signal 104 is periodically sampled 202. (Page 8, lines 2-4)
hashing means coupled to said selection means for hashing the set of data into a keyword.	And, a hashing module receives and hashes the set of data into a keyword. (Page 4, lines 6-7) a hashing module coupled to receive and hash the set of data into a keyword. (Original Claim 1 lines 7-8, Page 14)

Claim 24	Specification & Drawings

24. A computer-useable medium embodying computer program code adapted for use for multimedia encryption by executing the steps of:

Figure 1 is a block diagram of a system 100 for multimedia encryption according to the present invention. (Page 7, lines 2-3)

acquiring a random noise only media signal, said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;

In one embodiment of the present invention, the media signal need onl include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such a white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods. (Page 7, lines 10-15)

compressing said random noise only media signal, said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;

The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108. (Page 7, lines 19-22)

selecting a set of data from the compressed media signal; and

Figure 2 is a graphical depiction of quantization processes within the analog-to-digital converter 106 within the system 100. The media signal 104 is periodically sampled 202. (Page 8, lines 2-4)

hashing the set of data into a keyword.

And, a hashing module receives and hashes the set of data into a keyword. (Page 4, lines 6-7) a hashing module coupled to receive and hash the set of data into a keyword. (Original Claim 1 lines 7-8, Page 14)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Final Rejection mailed April 25, 2008 states three grounds of rejection. The three grounds of rejection are summarized below.

Grounds of Rejection #1 - Claims 1-30 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. The rejection is stated in numbered paragraph 3 on pages 2-5 of the Final Rejection mailed April 25, 2008.

Grounds of Rejection #2 - Claims 1-30 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellants regards as the invention. The rejection is stated in numbered paragraph 5 on page 5 of the Final Rejection mailed April 25, 2008.

Grounds of Rejection #3 - Claims 1-30 were rejected under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential steps, elements or instructions. The rejection is stated in numbered paragraph 6 on pages 5 and 6 of the Final Rejection mailed April 25, 2008.

VII. ARGUMENT

Argument Relating to Grounds of Rejection #1 - Appellants' claims 1-30 comply with the written description requirement. It is clear from Appellants' original specification that a person skilled in the art would recognize the inventor(s) had possession of the claimed invention including the claim limitation "random noise being unpredictable from one moment to the next" of claims 1, 10, 17, and 24. Appellants' specification discusses and describes "random noise" throughout the application.

Appellants' specification on pages 4 and 5 states: "The system/apparatus and method of the present invention are particularly advantageous over the

prior art because a means of capturing random numbers for encryption seeding directly from variable frame boundary compressed data is disclosed. In light of a growing importance in securely transmitting multimedia data over digital networks, obtaining random numbers directly from the multimedia data would be very useful."

Appellants' specification on page 7, lines 10-15 states: "In one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods."

Appellants' specification in connection with FIG. 2 states, "The random noise in the media signal 104 will cause even unchanging video scenes to have quantization values 206 which fluctuate for media signal values close to one or more quantization steps 204. ..... Typically, the transducer noise is sufficient to cause the quantization values 206 to fluctuate. However, if the transducer noise is small relative to the quantization steps 204, then either video or audio content of the media signal 104 must vary somewhat so that what little noise is in the scene will enable random noise to be quantized by the A/D converter 106. Randomness will be present in the media signal 104 when an actual sampled media signal value 208 is very close to a quantization boundary 210."

Inventor(s) Had Possession of Claimed Invention

A person skilled in the art would recognize that the inventor had possession of the claimed invention including the claim limitation "random noise being unpredictable from one moment to the next" of claims 1, 10, 17, and 24. The concepts and fundamentals of "random noise" were well known in the prior art at the time Appellants filed their patent application. For example, the

October 16, 1998 publication "DESIGN OF RANDOM NOISE GENERATOR USING SW ALGORITHM" by Jinkeun Hong, Sunchun Park, Janghong Yoon, Jaeyoung Koh, and Daeho Kim and the publication cited in the article describe. concepts and fundamentals of "random noise." A copy of the publication is provided in the EVIDENCE APPENDIX (IX).

Person Skilled In The Art

The level of skill of a person skilled in the relevant art is very high. It includes scientists with BS degrees in electrical engineering or computer sciences and advanced degrees in electrical engineering or computer sciences. The lead inventor, Douglas R. Coffland, is Division Leader - Security Engineering and Computation Division of the Lawrence Livermore National Laboratory. The Lawrence Livermore National Laboratory (LLNL) is a premier applied science laboratory that is part of the National Nuclear Security Administration (NNSA) within the Department of Energy (DOE). The LLNL website states that LLNL employs 6,600 full-time employees, including 2,681 scientists and engineers of which 1,212 hold Ph.D degrees. The *Wikipedia, the free encyclopedia* describes the Lawrence Livermore National Laboratory. A copy of the *Wikipedia, the free encyclopedia* description of the Lawrence Livermore National Laboratory is provided in the EVIDENCE APPENDIX (IX).

The Lawrence Livermore National Laboratory computer operations are the best in the world. According to recent TOP500 lists, Computation operates some of the world's fastest supercomputers: BlueGene/L, a cooperative project to design and build a computer architecture capable of scaling to hundreds of teraflops (TF); ASC Purple, a genuinely huge machine based on symmetric shared-memory multiprocessors containing more than 12,000 next-generation IBM Power5 microprocessors and capable of 100 TF; and Thunder (right), a highly integrated, well-balanced capability compute resource with 1,024 nodes

and a theoretical system peak performance of 22.9 TF. A copy of two pages from the Lawrence Livermore National Laboratory website www.llnl.gov is provided in the EVIDENCE APPENDIX (IX).

Encryption is of high importance to the National Nuclear Security Administration (NNSA), the Department of Energy (DOE), and the Lawrence Livermore National Laboratory. The lead inventor, Douglas R. Coffland, as Division Leader - Security Engineering and Computation Division of the Lawrence Livermore National Laboratory is highly skilled in Encryption. The lead inventor, Douglas R. Coffland, as Division Leader - Security Engineering and Computation Division of the Lawrence Livermore National Laboratory had possession of the claimed invention including the claim limitation "random noise being unpredictable from one moment to the next" of claims 1, 10, 17, and 24.

Appellants' Specification Supports Claim Limitation

Appellants' specification taken as a whole supports the claim limitation. MPEP § 2163 II.A.3 states, "An adequate written description of the invention may be shown by any description of sufficient, relevant, identifying characteristics so long as a person skilled in the art would recognize that the inventor had possession of the claimed invention."

Presumption of Adequate Written Description

There is a strong presumption that an adequate written description of the claimed invention is present when the application is filed. In re Wertheim, 541 F.2d 257, 263, 191 USPQ 90, 97 (CCPA 1976), the implication stated in the Final Rejection is contradicted by Appellants' specification taken as a whole. The implication stated in the Final Rejection is not sufficient to overcome the presumption that an adequate written description of the claimed invention is present when the application is filed.

Written Description Rejection Should Be Reversed

The rejection of claims 1-30 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement should be reversed.

Argument Relating to Grounds of Rejection #2 – The Final Rejection mailed April 25, 2008 and previous office actions do not explain why claims 1-30 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention.

Appellants' claims 1-30 comply with the requirements of 35 U.S.C. § 112, second paragraph.

Appellants' Claims Point Out and Distinctly Claim Invention

Appellants' claimed invention defined by independent claim 1 is "a system adapted for use for multimedia encryption." Claim 1 includes a combination of structural elements that produce the system adapted for use for multimedia encryption. The structural elements include "acquisition means for acquiring a media signal," "data compression means coupled to said acquisition means to receive and compress said media signal," "data acquisition means coupled to said data compression means to receive and select a set of data from the compressed data stream," and "hashing means coupled to said data acquisition means to receive and hash the set of data into a keyword." These structural elements produce the system adapted for use for multimedia encryption. Appellants' submit that claim 1 describes the invention sufficiently and particularly points out and distinctly claims the subject matter which Appellant regards as the invention and claim 1 meets the requirements of 35 U.S.C. § 112, second paragraph.

Appellants' claimed invention defined by independent claim 10 is "a method adapted for use for multimedia encryption." Claim 10 includes a

combination of steps. The steps include "acquiring a random noise only media signal," "compressing said random noise only media signal," "selecting a set of data from the compressed media signal," and "hashing the set of data into a keyword." Appellants' submit that claim 10 describes the invention sufficiently and particularly points out and distinctly claims the subject matter which Appellant regards as the invention and claim 10 meets the requirements of 35 U.S.C. § 112, second paragraph.

Appellants' claimed invention defined by independent claim 17 is "a system adapted for use for multimedia encryption." Claim 17 includes a combination of structural elements that produce the system adapted for use for multimedia encryption. The structural elements include "acquisition means for acquiring a media signal," "data compression means coupled to said acquisition means to receive and compress said media signal," "selection means coupled to said data compression means for selecting a set of data from the compressed data stream," and "hashing means coupled to said selection means for hashing the set of data into a keyword." These structural elements produce the system adapted for use for multimedia encryption. Appellants' submit that claim 17 describes the invention sufficiently and particularly points out and distinctly claims the subject matter which Appellant regards as the invention and claim 17 meets the requirements of 35 U.S.C. § 112, second paragraph.

Appellants' claimed invention defined by independent claim 24 is "a computer-useable medium embodying computer program code adapted for use for multimedia encryption by executing the steps." Claim 24 includes a combination of steps. The steps include "acquiring a random noise only media signal," "compressing said random noise only media signal," "selecting a set of data from the compressed media signal," and "hashing the set of data into a keyword." The steps produce the computer-useable medium embodying

computer program code adapted for use for multimedia encryption. Appellants' submit that claim 24 describes the invention sufficiently and particularly points out and distinctly claims the subject matter which Appellant regards as the invention and claim 24 meets the requirements of 35 U.S.C. § 112, second paragraph.

35 U.S.C. § 112, Second Paragraph Rejection Should Be Reversed

The rejection of claims 1-30 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention should be reversed.

Argument Relating to Grounds of Rejection #3 – Appellants' claims 1-30 do not omit essential steps.

Independent Claim 1

Appellants' claimed invention defined by independent claim 1 is "a system adapted for use for multimedia encryption." Claim 1 includes a combination of structural elements that produce the system adapted for use for multimedia encryption. The structural elements include "acquisition means for acquiring a media signal," "data compression means coupled to said acquisition means to receive and compress said media signal," "data acquisition means coupled to said data compression means to receive and select a set of data from the compressed data stream," and "hashing means coupled to said data acquisition means to receive and hash the set of data into a keyword." These structural elements produce the system adapted for use for multimedia encryption. There are no essential structural elements omitted. Appellants' submits that claim 1 is not incomplete for omitting essential elements, and claim 1 meets the requirements of 35 U.S.C. § 112, second paragraph.

Independent Claim 10

Appellants' claimed invention defined by independent claim 10 is "a method adapted for use for multimedia encryption." Claim 10 includes a combination of steps. The steps include "acquiring a random noise only media signal," "compressing said random noise only media signal," "selecting a set of data from the compressed media signal," and "hashing the set of data into a keyword." There are no essential steps omitted. Appellants' submits that claim 10 is not incomplete for omitting essential steps, and claim 10 meets the requirements of 35 U.S.C. § 112, second paragraph.

Independent Claim 17

Appellants' claimed invention defined by independent claim 17 is "a system adapted for use for multimedia encryption." Claim 17 includes a combination of structural elements that produce the system adapted for use for multimedia encryption. The structural elements include "acquisition means for acquiring a media signal," "data compression means coupled to said acquisition means to receive and compress said media signal," "selection means coupled to said data compression means for selecting a set of data from the compressed data stream," and "hashing means coupled to said selection means for hashing the set of data into a keyword." These structural elements produce the system adapted for use for multimedia encryption. There are no essential structural elements omitted. Appellants' submits that claim 17 is not incomplete for omitting essential elements, and claim 17 meets the requirements of 35 U.S.C. § 112, second paragraph.

Independent Claim 24

Appellants' claimed invention defined by independent claim 24 is "a computer-useable medium embodying computer program code adapted for use for multimedia encryption by executing the steps." Claim 24 includes a

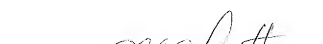
combination of steps. The steps include "acquiring a random noise only media signal," "compressing said random noise only media signal," "selecting a set of data from the compressed media signal," and "hashing the set of data into a keyword." The steps produce the computer-useable medium embodying computer program code adapted for use for multimedia encryption. There are no essential steps omitted. Appellants' submits that claim 24 is not incomplete for omitting essential steps, and claim 24 meets the requirements of 35 U.S.C. § 112, second paragraph.

Omitting Essential Steps Rejection Should Be Reversed

The rejection of claims 1-30 under 35 U.S.C. § 112, first paragraph, as allegedly being incomplete for omitting essential steps, elements or instructions should be reversed.

It is respectfully requested that claims 1-30 on appeal be allowed.

Respectfully submitted,

By: 

Eddie E. Scott
Lawrence Livermore National Laboratory
7000 East Avenue, Mail Code L-703
Livermore, CA 94550
Attorney for Appellants
Registration No. 25,220
Telephone No. (925) 424-6897

Date: February 5, 2009

VIII. CLAIMS APPENDIX

1. A system adapted for use for multimedia encryption comprising:

acquisition means for acquiring a media signal, said acquisition means including a random noise transducer for acquiring random noise only, said random noise being unpredictable from one moment to the next and not being chaotic noise;

data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise into a compressed data stream;

data acquisition means coupled to said data compression means to receive and select a set of data from the compressed data stream; and

hashing means coupled to said data acquisition means to receive and hash the set of data into a keyword.

2. The system of claim 1 wherein the set of data is one frame of data within the compressed data stream.

3. The system of claim 1 wherein the set of data crosses over several frame boundaries within the compressed data stream.

4. The system of claim 1 wherein: the compressed data stream includes compression transform coefficients; and the set of data includes a set of compression transform coefficients.

5. The system of claim 1 wherein: the compressed data stream includes data frames of varying length; and the set of data includes a set of data frames.

6. The system of claim 1 wherein: the compressed data stream includes predictive data frames; and the set of data includes a predictive data frame.

7. The system of claim 1: wherein the media signal includes a noise signal amplitude; further comprising, an analog to digital converter, having a

quantization step size smaller than the noise signal amplitude, coupled to receive and quantize the media signal; and wherein the data compression module compresses the quantized media signal into a compressed data stream.

8. The system of claim 1 wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats.

9. The system of claim 1 further comprising: a pseudo-random number generator coupled to receive and process the keyword in to a set of keywords.

10. A method adapted for use for multimedia encryption, comprising the steps of:

acquiring a random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;

compressing said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;

selecting a set of data from the compressed media signal; and

hashing the set of data into a keyword.

11. The method of claim 10 wherein: the compressed media signal includes data frames; and the selecting step includes the step of selecting one frame of data.

12. The method of claim 10 wherein: the compressed media signal includes data frames and data frame boundaries; and the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries.

13. The method of claim 10 wherein: the compressed media signal includes compression transform coefficients; and the selecting step includes the step of selecting a set of compression transform coefficients.

14. The method of claim 10 wherein: the compressed media signal includes data frames of varying length; and the selecting step includes the step of selecting a set of data frames.

15. The method of claim 10 wherein: the compressed media signal includes predictive data frames; and the selecting step includes the step of selecting a predictive data frame.

16. The method of claim 10: wherein the media signal includes a noise signal amplitude; further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude; and wherein the compressing step includes the step of compressing the quantized media signal.

17. A system adapted for use for multimedia encryption, comprising:

acquisition means for acquiring a media signal, said acquisition means including a random noise transducer for acquiring said media signal, said random noise transducer acquiring said media signal containing only random noise that is unpredictable from one moment to the next and not being chaotic noise;

data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is unpredictable from one moment to the next into a compressed data stream;

selection means coupled to said data compression means for selecting a set of data from the compressed data stream; and

hashing means coupled to said selection means for hashing the set of data into a keyword.

18. The system of claim 17 wherein: the compressed media signal includes data frames; and the means for selecting includes means for selecting one frame of data.

19. The system of claim 17 wherein: the compressed media signal includes data frames and data frame boundaries; and the means for selecting includes means for selecting a set of data which crosses over several data frame boundaries.

20. The system of claim 17 wherein: the compressed media signal includes compression transform coefficients; and the means for selecting includes means for selecting a set of compression transform coefficients.

21. The system of claim 17 wherein: the compressed media signal includes data frames of varying length; and the means for selecting includes means for selecting a set of data frames.

22. The system of claim 17 wherein: the compressed media signal includes predictive data frames; and the means for selecting includes means for selecting a predictive data frame.

23. The system of claim 17: wherein the media signal includes a noise signal amplitude; further comprising means for quantizing the media signal with a quantization step size smaller than the noise signal amplitude; and wherein the means for compressing includes means for compressing the quantized media signal.

24. A computer-useable medium embodying computer program code adapted for use for multimedia encryption by executing the steps of:

acquiring a random noise only media signal, said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;

compressing said random noise only media signal, said random noise only media signal containing random noise that is unpredictable from one moment to the next and not being chaotic noise;

selecting a set of data from the compressed media signal; and

hashing the set of data into a keyword.

25. The computer-useable medium of claim 24 wherein: the compressed media signal includes data frames; and the selecting step includes the step of selecting one frame of data.

26. The computer-useable medium of claim 24 wherein: the compressed media signal includes data frames and data frame boundaries; and the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries.

27. The computer-useable medium of claim 24 wherein: the compressed media signal includes compression transform coefficients; and the selecting step includes the step of selecting a set of compression transform coefficients.

28. The computer-useable medium of claim 24 wherein: the compressed media signal includes data frames of varying length; and the selecting step includes the step of selecting a set of data frames.

29. The computer-useable medium of claim 24 wherein: the compressed media signal includes predictive data frames; and the selecting step includes the step of selecting a predictive data frame.

30. The computer-useable medium of claim 24: wherein the media signal includes a noise signal amplitude; further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude; and wherein the compressing step includes the step of compressing the quantized media signal.

IX. EVIDENCE APPENDIX

1. October 16, 1998 publication "DESIGN OF RANDOM NOISE GENERATOR USING SW ALGORITHM" by Jinkeun Hong, Sunchun Park, Janghong Yoon, Jaeyoung Koh, and Daeho Kim

2. *Wikipedia, the free encyclopedia* description of the Lawrence Livermore National Laboratory

3. Two pages from the Lawrence Livermore National Laboratory website *www.llnl.gov*

X. RELATED PROCEEDINGS APPENDIX

There are no entries in the Related Proceedings Appendix.

DESIGN OF RANDOM NOISE GENERATOR USING SW ALGORITHM

Jinkeun Hong[*], Sunchun Park*, Janghong Yoon[*], Jaeyoung Koh[*], Daeho Kim[*]
[*]National Security Research Institute, 161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, KOREA
JKHONG1024@ETRI.RE.KR

ABSTRACT

A random noise generator uses a non-deterministic source to produce randomness. Most operate by measuring unpredictable natural processes, such as thermal noise, atmospheric noise, or nuclear decay. Critical cryptography applications require the production of an unpredictable and unbiased stream of binary data derived from a fundamental noise mechanism. In this paper, we proposed a random noise generator with Gaussian noise using filtering algorithm. The proposed scheme is designed to reduce the statistical property of the biased bit stream in the output of a random noise generator.

Keywords: *Random Noise generator, Gaussian Noise Source, randomness.*

1. INTRODUCTION

More demanding random noise applications, such as cryptography and statistical simulation, benefit from sequences produced by a random noise generator, a cryptographic system based on a hardware component [1]. A real noise generator is a source of unpredictable, irreproducible, and statistically random stream sequences. A popular method for generating random numbers using a natural phenomenon is the electronic amplification and sampling of a thermal or Gaussian noise signal. Since all electronic systems are influenced by a finite bandwidth, 1/ f noise, and other non-random influences, perfect randomness cannot be preserved by any practical system. Thus, when generating random numbers using an electronic circuit, a low-power white noise signal is amplified, and then sampled at a constant sampling frequency. However, it is quite difficult to create an unbiased and stable random bit stream, as required for statistical randomness, when using a random generator with only a hardware component. The studies reported in [2-4] show that the randomness of a random stream can be enhanced when combining a random noise generator and hash function (or LFSR). However, the randomness of this combined method is still dependent on the security level of the hash function (or LFSR). Accordingly, the current paper proposes a random noise generator that combines a random noise generator and filtering technique that is not dependent on the security level of the period. First, the proposed random noise generator is introduced, followed by the hardware system. Finally, experimental results using the proposed system are presented.

2. DESIGN FOR PROPOSED REAL RANDOM NOISE GENERATOR

Random noise generators include common components for producing random bit-streams, classified as follows: characteristics of the noise source, amplification of the noise source, and sampling for gathering the comparator output.

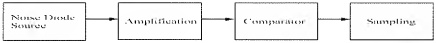


Fig.1. Random Noise generator

2.1 Characteristics of Noise Source

The applied noise source uses Gaussian noise, which typically results from the flow of electrons through a highly charged field, such as a semiconductor junction. Ultimately, the electron flow is the movement of discrete charges, and the mean flow rate is surrounded by a distribution related to the launch time and momentum of the individual charge carriers entering the charged field. The Gaussian noise generated in a PN junction has the same mathematical form as that of a temperature-limited vacuum diode. The noise seems to be generated by the noise current generator in parallel with the dynamic resistance of the diode.

$$I_{ns} = (2 e I_{dc} B)^{1/2} \quad (1)$$

Where e= Electron charge (1.6×10^{-19} coulombs), I_{dc}= Average dc current (A), B=Noise bandwidth (Hz). The Gaussian noise voltage can be determined by applying Ohms Law.

$$E_{ns} = (2 e I_{dc} B r_d^2)^{1/2} \quad (2)$$

Where, r_d is the dynamic resistance of the junction.

It is known that the dynamic resistance of a PN junction depends on the temperature and direct current flowing through the junction. The dynamic resistance represents the ratio of a small change in the diode voltage to the corresponding change in the diode current.

$$r_d = kT/eI_{dc} \quad (3)$$

Substituting produces

$$E_{ns} = (2kTBr_d)^{1/2} \quad (4)$$

Substituting again produces

$$E_{ns} = kT(2/eI_{dc})^{1/2} \quad (5)$$

Where K = Boltzmanns constant (1.38×10^{-23} Joules/deg. Kelvin), T = Temperature in degrees Kelvin, B = Bandwidth in Hertz, r_d = dynamic resistance, and e = Electron charge (1.6×10^{-19} coulombs). The dynamic resistance is inversely proportional to the direct current and decreases as the direct current increases, thereby causing the Gaussian noise voltage across the junction to decrease. Yet, if the direct current increases, the dynamic resistance decreases more quickly than the Gaussian noise current increases. As such, the Gaussian noise voltage becomes inversely related to the direct current. However, for the proposed random noise generator, the noise diode is a Zener diode with a white Gaussian distribution. The noise power density remains constant with a frequency from 0.1Hz to 10MHz and the amplitude has a Gaussian distribution. The noise must be amplified to a level where it can be accurately thresholded with no bias using a clocked comparator. The applied voltage is ±15Vdc and the current-limiting resistor is 16KΩ. The frequency range is 0.1Hz to 10MHz and the noise output is 0.1uV/√Hz (min.). The noise diode breakdown voltage is 7V to 10V.

2.2 Amplification of Noise Source

The amplification technique [5] uses a high-gain, high-bandwidth amplifier to amplify the small ac voltage produced by a thermal or Gaussian noise source.

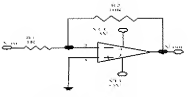


Fig. 2. Schematic Drawing of Amplifier

The noise must be amplified to a level where it can be accurately thresholded with no bias using a clocked comparator. The amplifiers operate from ±5V supplies. C_1 and C_2 are the power supply bypass capacitors. C_3 helps to prevent peaking at high frequencies. This peaking results from the input capacitance of the OP Amplifier, which is driven by the relatively high impedance of the feedback resistors, R_1 and R_2.

2.3 Sampling and filtering for gathering comparator output

When the output of a fast oscillator is sampled on the rising edge of a slower reference clock, the comparator features differential analog inputs and TTL logic outputs with an active internal pull-up and supplies a fast propagation delay for the sampling circuits. The applied voltage is ±5Vdc and propagation delay is 8nsec. The frequency range can be stably operated up to 100MHz. First, the sampled stream is gathered, then a filtering algorithm is used to enhance the statistical randomness. The filtering algorithm provides a stable random bit stream instead of a biased and faulted stream. Generally, since the randomness of the bit stream from the random noise generator can not be continuously guaranteed, the random noise generator guarantees the security level performance using a filtering algorithm, which resolves the problem of an unbiased, unstable random bit stream.

3. CHARACTERISTICS OF PROPOSED SYSTEM

3.1 Implemented Architecture and Environment

Basic simulation models were created for the common RNG methods to track the effects of topological design decisions and key circuit parameters on randomness. These models produced binary sequences, which were checked for randomness using accepted statistical randomness tests. Ten minutes is required to gather stable White GAUSSIAN random noise from a ZENER diode noise source. The proper amplitude for the amplification noise voltage should be about 1Volt to reduce the effect of bias. Based on equation (1), the diode current slightly fluctuates at the center of the level, which is based on the DC value. The RMS value of the Gaussian noise due to a drift current(DC) of 0.3mA is about $1uA/Hz^{1/2}$ [$=2 \bullet 1.6 \bullet 10^{-19} \bullet 0.3 \bullet 10^{-3}$]. The output waveform of the diode stage represents the spectrum density with a white noise frequency distribution and instantaneous amplitude with a Gaussian distribution. The collected AC signal, which is the output of the filter stage using HPF, without a DC signal, is applied as the noise source. The determination of the low cut-off frequency required for gathering the effective random bit stream is as follows:

$$f_c = 1 / 2 \bullet Pi \bullet R \bullet C \qquad (6)$$

Where Pi = 3.14, R is the resistor, and C is the capacitor. Therefore, the value of f_c is 1/[2 • 3.14 • 2.4K • 0.00015E-6] = 442.1KHz. Thus, the available frequency range is from 442KHz to 10GHz. From Figure (2), the voltage gain (Av) of the inverse amplifier of the noise source is as follows:

$$Av = V0 / Vi = -R1 / R2 \qquad (7)$$

Where R1=10K and R2=1K. Thus, the voltage gain (Av) can be amplified by a multiple of 10 of the input noise source, as presented in Figure (2).

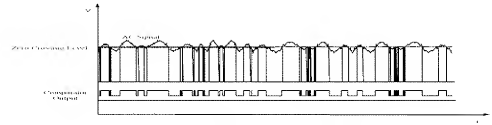


Fig.3. Comparison of Comparator Stage and Amp Stage

The comparator is decided by the zero crossing level. The variation in the voltage level of the noise source, which is based on the zero crossing point, is due to the transition of the output voltage state. The output of the comparator is sampled at the sampling rate. Determining the sampling rate for the sampler is important, because the statistical randomness of the output stream of a random bit "0/1" is dependent on the reference clock rate of the comparator and sampling rate of the sampler. The sampling rate applied to the sampler is a clock rate 1/30 slower than the reference clock rate for the comparator. As a result, the sampler collects an unbiased random bit stream.

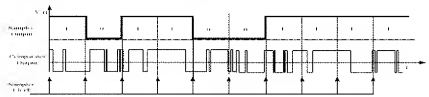


Fig.4. Output of Sampler

3.2 Filtering Algorithm

An filtering algorithm is applied in the next process of the output stream of the sampler to reduce the biased statistical randomness. If the optimum buffer size [64bits] and significance level [P] are established, this supports unbiased and stable randomness.

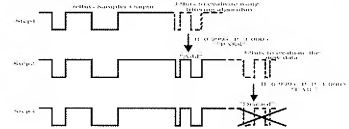


Fig. 5. Process of filtering algorithm

In the current paper, a static buffer memory of 64bits is used to buffer the "pass data" in the decision boundary and the significance level for the P value is between 0.9995 and 1.0005.

$$P = \frac{\text{the sum of number of '1' bit Total Sum}}{\text{the half value of the static length Total Length}} \tag{8}$$

When the static buffer is fixed at 64bits, the half-value of the static length is 16 bits. If the value of {Σ{the number of a pattern' 1' bit} / the half-value of the static length within the total length} is included in the significance level, the decision will be "pass". In step 1, if "pass" is decided, this is added as pass

data to the buffer memory. In step 3, if "fail" is decided, this is discarded as failed data. The process is then completed when the size of the desired bit stream is gathered.

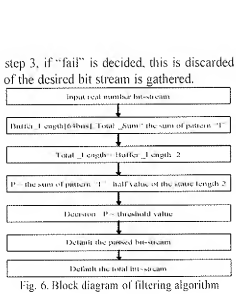


Fig. 6. Block diagram of filtering algorithm

3.3 Experimental Results

This section presents the results obtained from the proposed system. First, the effect of the randomness of the output random bit stream was investigated. More quantitative tests for randomness can be found in technical literature [6-7]. In Figures 8 – 11 represent various randomness tests along with their references, typical pass/fail boundaries, the measured average of 20 iteration tests based on 8MB samples, and whether the sequence passed all the trial tests. The test results were extremely positive: i.e. the proposed system passed all the trial tests. The proposed system was able to generate an 8MB data size within 7minutes. The direct line in the graph is the threshold value for making a decision. If the evaluation level goes above the threshold level, the decision will be "fail".

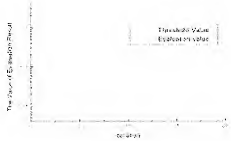


Fig. 6. Evaluation Value for Frequency Test

Fig. 7. Evaluation Value for Serial Test

Fig. 8. Evaluation Value for T-Serial Test

Fig. 9. Evaluation Value for Poker Test

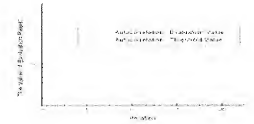


Fig. 10. Evaluation Value for Autocorrelation Test

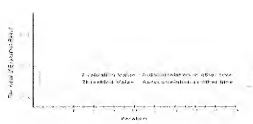


Fig. 11 Evaluation Value for Autocorrelation Test with another time

Figures 6-10 present the evaluation results for each item. Figure 11 shows a comparison of the evaluation value of a gathered bit stream with another time, demonstrating that the evaluation value was not correlated with itself or with another time. Accordingly, the graphs clearly illustrate that the evaluation value of the random bit stream was smaller than the threshold value. Although the current results only represent intuitive randomness, the proposed model is expected to be useful in a random noise generator.

4. CONCLUSION

The current paper presented and tested a random noise generator using Gaussian noise. The proposed method, directly derived from results obtained from the Gaussian noise generator, is based on filtering a white noise sequence using a software filter. The Gaussian noise generator concept can be applied to any IC process where a Zener diode is available. The random noise generator is well suited for applications such as data encryption, circuit testing and measurement, and mathematical simulations. With further improvements to the design of the random noise generator components, even faster data gathering can be achieved.

REFERENCES

[1] C. S. Petrie and J. A. Connelly, "A Noise-Based Random Bit Generator IC for Applications in Cryptography," Proc. ISCAS'98, June 1998.

[2] http://www.io.com/~ritter/R3SNOISE.HTM

[3] http://www.clark.net/pub/cme/P136j/zonno.html.

[4] http://webviz.com/robert.trug.rng.html.

[5] W. Timothy Holman, J. Alvin Connelly, and Ahmad B. Dowlatabadi, "An Integrated Analog Digital Random Noise Source," IEEE Transactions on Circuits and System I: Fundamental Theory and Applications, Vol.44, No.6, June 1997.

[6] FIPS 140-1, "Security Requirements for Cryptographic Modules," [Federal Information Processing Standards Publication 140-1], U.S. Department of Commerce/NIST[National Technical Information Service] Springfield, Virginia,1994.http://csrc.ncsl.nist.gov/fips/fips1401.htm (16 Oct. 1998).

[7] "Diehard," http://stat.fsu.edu/~geo/diehard.html (16 Oct. 1998).

Lawrence Livermore National Laboratory

From Wikipedia, the free encyclopedia

The **Lawrence Livermore National Laboratory** (**LLNL**) is a United States Department of Energy (**DOE**) national laboratory, managed and operated by the University of California, in Livermore, California until September 30, 2007. As of October 1, 2007 the lab will be managed by Lawrence Livermore National Security, LLC (LLNS), a consortium comprised of the University of California, Bechtel National, BWX Technologies, Washington Group International, and Battelle Memorial Institute. Along with Los Alamos National Laboratory in New Mexico, it is one of the two United States laboratories whose founding mission was the design of nuclear weapons.

LLNL is self-described as "a premier research and development institution for science and technology applied to national security."[1] It is responsible for ensuring that the nation's nuclear weapons remain "safe, secure, and reliable" through application of advances in science, engineering, and technology. The laboratory also applies its special expertise and multidisciplinary capabilities to preventing the proliferation and use of weapons of mass destruction, and to bolstering homeland security. Those capabilities are also utilized in programs in non-defense areas such as basic science, energy, environmental science, and biosciences.

Lawrence Livermore National Laboratory

Motto	"Science in the national interest"
Established	1952
Research Type	National security and basic science
Budget	$1.6 billion/year
Director	George H. Miller
Staff	9,600 (100) (United States Department of Energy)
Location	Livermore, CA
Campus	800 acres (3.2 km²)
Operating Agency	University of California
Website	www.llnl.gov (http://www.llnl.gov/)

LLNL is home to many of the most powerful computer systems in the world, according to the TOP500 list, including Blue Gene/L, the world's fastest computer as of 2005. Since 1978 the laboratory has received a total of 113 prestigious R&D 100 Awards, including seven in 2006, the most for any institution.[2] The awards are given annually by the editors of R&D Magazine (http://www.rdmag.com/) to the most innovative ideas of the year.

Aerial view of the lab and surrounding area, facing NW.

LLNL's main facility is located on a one-square-mile (2.6 km^2) site at the eastern outskirts of Livermore, California. Site 300, a 7,000-acre (28.3 km^2) remote explosive/experiment testing site, is situated about 15 miles (24 km) to the southeast. Lawrence Livermore has an annual budget of about $1.6 billion and a staff of over 8,000 University of California employees, as well as 1,500 contract employees. Additionally, there are approximately 100 DOE employees stationed at the laboratory to provide federal oversight of LLNL's work for the DOE.

Lawrence Livermore National Laboratory

About LLNL

Facts & Figures
Laboratory Values
Management & Sponsors
Institutional Publications
Laboratory Operations
Ties to the Community
History

Lawrence Livermore National Laboratory (LLNL) is a pre laboratory that is part of the National Nuclear Security Ac within the Department of Energy (DOE). LLNL has been inception in 1952 by the University of California for the U.

As a national security laboratory, LLNL is responsible for ensuring that the nation's nuclear weapons remain safe, secure, and reliable through application of advances in science and engineering. With its special capabilities, the Laboratory also meets other pressing national security needs, which include countering the proliferation of weapons of mass destruction and strengthening homeland security against the terrorist use of such weapons.

Our breakthrough advances are made possible by an extraordinary technical staff and investments in research facilities that provide LLNL wide ranging capabilities. The Laboratory is an international leader in many areas of science and technology central to ou national security mission.

With our broadly based capabilities and leadership in mission-fo and engineering, the Laboratory is able to also make major adva national needs. LLNL pursues major research programs in energ bioscience and biotechnology, and basic science and advanced

The Laboratory is able to attract a superb workforce because of i and opportunities to pursue leading-edge research as part of mu This keeps the Laboratory at the forefront of technical capabilitie national security mission and ready to effectively respond to evol national priorities and surprises.

Lawrence Livermore has an annual budget of about $1.6 billion and a staff of over 8,000 er over 3,500 scientists, engineers, and technicians together with professionals in many other Laboratory running in a safe, secure and efficient manner.

Director's Office
Administration & Human Resources
Chief Financial Officer
Chemistry, Materials, & Life Sciences
Computation
Defense & Nuclear Technologies
Energy & Environment
Engineering
Laboratory Services
National Ignition Facility
Nonproliferation, Homeland and International Security
Physics & Advanced Technologies
Safeguards & Security
Safety & Environmental Protection

Home : Organization :: **Computation**

Computation Directorate

- **Computation Directorate Website**
- **Associate Director's Bio**

Since 1952, Laboratory scientists and engineers have relied on the m simulation environments for science in the national interest.

Computation offers computing capacity and capability in support of the nation's Stockpile St This makes Computation a key partner in the Advanced Simulation and Computing (ASC) p known as ASCI. Computation also provides unclassified computing capacity and capability Multiprogrammatic & Institutional Computing (M&IC).

According to recent TOP500 lists, Computation operates some of the world's fastest supercomputers: BlueGene/L, a cooperative project to design and build a computer architecture capable of scaling to hundreds of teraflops (TF); ASC Purple, a genuinely huge machine based on symmetric shared-memory multiprocessors containing more than 12,000 next-generation IBM Power5 microprocessors and capable of 100 TF; and Thunder (right), a highly integrated, well-balanced capability compute resource with 1,024 nodes and a theoretical system peak performance of 22.9 TF.